إجراءات جمع الأدلة
في مجال جريمة سرقة المعلومات

الرائد الدكتور عبد ا حسين علي محمود

** المقدمة

إن ظاهرة جرائم الحاسب الآلي، ظاهرة إجرامية جديدة مستحدثة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الحاسب الآلي التي تستهدف الإعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها).

فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

وتنبع أهمية هذا الموضوع من دور الثورة المعلوماتية في عملية التنمية الشاملة بنوعيها الإقتصادي والإجتماعي وحاجتها من ثم إلى بحث المشكلات القانونية المتعلقة بها ومحاولة الوصول إلى إيجاد الحلول المناسبة لها.

ومن ناحية أخرى، فإن المعلوماتية بإعتبارها ظاهرة إنسانية وإقتصادية وإجتماعية لا يمكن أن تتطور بذاتها دون أن تتوافر لها القواعد القانونية التي تنظم استغلالها.

وأصبح الحاسب الآلي على مدى الفترة الماضية ركيزة أساسية لأهداف التطور في شتى مناحي الحياة، سواء تمثلت في أنشطة اقتصادية أو علمية أو صناعية أو زراعية.

وترتب على الإستخدام المتزايد لنظم المعلومات سواء في شكل أموال معلوماتية " biens informatiques أو أساليب مستحدثة إلى نشوء ما يعرف بالجريمة المعلوماتية، وهي نتيجة حتمية لكل تطور علمي أو تقني مستحدث، ويرتكن هذا النوع من الإجرام على محوريين أولهما ضد المال والثاني ضد الأشخاص ويستمد نشاطه من القدارت الهائلة من الحاسب الآلي[1].

ويرى الأستاذ Parker أن الجريمة المعلوماتية (كل فعل إجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسبا يحققه الفاعل)[2].

---

1 Masse (M) Emergence du dioit de Linformatique, ed des parques 1983, p.21
2 D.B. parker, combattre la crimpinalite informatique, Ed Otos 1985, p. 18.



بينما يرى خبراء المنظمة الأوروبية للتعاون والتنمية الإقتصادية أن المقصود بالجريمة المعلوماتية هي (كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به، يرتبط بالمعالجـة الآليـة للبيانـات أو بنقلها)[3].

ويجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغـش المعلومـاتي Fraude informatique التي تعادل جريمة الكمبيوتر computer related crime anglo saxon وهي تشمل العديد من عدة أفعال متنوعة وليس المقصود بها وصفا ولكنها بالأحرى ينظر إلى هذا المصطلح بوصـفه مـصطلحا خاصا بعلم الإجرام[4]، وهذا المصطلح يكتنفه غموض على قدر كبير وربما يكون له معان متعددة[5] لكي يمكن أن نحدد مجموعة قانونية مباشرة تطبق على مستوى القانون الجنائي.

وتتميز أفعال الجريمة المعلوماتية على نحو قليل في مضمونها وتنفيذها أو محـو آثارهـا عـن تلـك الخاصية بالجريمة التقليدية حيث يكفي للمجرم المعلوماتي أن يلمس لوحة مفاتيح الحاسب الآلي والتـي تقوم على الفوز بعمليات الحساب والتحليل وإسقاط الحواجز وأساليب الحماية الأكثر خداعا.

وأيضا تتميز جرائم الحاسب بالصعوبات البالغة في اكتشافها وبالعجز في حالات كثيرة عـن إمكـان اثباتها في حالة اكتشافها.

** ومرد ذلك الأسباب التالية:

- أولا: لا تخلف جرائم الحاسب آثارا ظاهرة خارجية فهي تنصب على البيانات والمعلومـات المختزنة في نظم المعلومات والبرامج مما ينفي وجود أي أثر مادي يمكن الإستعانة بـه فـي إثباتها، فالجرائم المعلوماتية ينتفي فيها العنف وسفك الدماء ولا توجد فيها آثار لإقتحام سـرقة الأموال، وإنما هي أرقام ودلالات تتغير أو تمحى من السجلات ومما يزيد من هذه الـصعوبة إرتكابها في الخفاء، وعدم وجود أثر كتابي مما يجري من خلال تنفيذها من عمليات حيث يتم نقل المعلومات بواسطة النبضات الإلكترونية.

---

3 O.C.D.E. Reunion de Paris, Mai 1983.

4 Champy, La fraude informatique these Aix en province 1990 p.58

5 يعرف Laura E. Quarantiello الجريمة المعلوماتية بأنها "عمل غير مشروع من شأنه استغلال ما ينتجه الحاسب بالمعرفة بغرض ارتكاب جريمة ما".
وهناك اربعة أنواع أساسية لتلك الأعمال غير المشروعة:
- الإستخدام غير المشروع لأجهزة الحاسب الآلي.
- ادخال بيانات أو سجلات مزورة في الحاسب الآلي.
- تدمير البيانات المعلوماتية.
- سرقة الخدمات أو البيانات المسجلة في الحاسب الآلي.

راجع في ذلك:
Laura E. Quarantiello. CYBER CRIME. P. 16 Ed Limelight.

• ثانيا: يتم إرتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل في مسرح الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة، وهذه المسافات لا تقف عند حدود الدولة بل تمتد إلى النطاق الإقليمي لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها.

• ثالثا: وتبدو أكثر المشكلات جسامة لا في مجال صعوبة إكتشاف وإثبات جرائم الحاسب بل وفي دراسة هذه الظاهرة في مجملها هي مشكلة امتناع المجني عليهم عن التبليغ عن الجرائم المرتكبة ضد نظام الحاسب وهو ما يعرف بالرقم الأسود Chiffrenoir[6]. حيث لا يعلم ضحايا هذه الجرائم شيئا عنها إلا عندما تكون أنظمتهم المعلوماتية هدفا لفعل الغش أو حتى عندما يعلمون فهم يفضلون عدم إفشاء الفعل[7].

ويلزم للمجتمع المعلوماتي في مجال قانون الإجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم الكمبيوتر.

والسبب في ذلك أن محترفي إنتهاك شبكات الحاسب الآلية ومرتكبي الجرائم الإقتصادية وتجار الأسلحة والمواد المخدرة يقومون بتخزين معلوماتهم في أنظمة تقنية المعلومات وعلى نحو متطور، وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكتيك لتخزين المعلومات وهي التي تسعى للحصول على أدلة الإثبات.

وتصادف الصعوبات عندما يتعلق الأمر على وجه الخصوص بتخزين بيانات بالخارج بواسطة شبكة الإتصالات البعدية Telecommunication[8] ويصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية للإكراه في قانون الإجراءات الجنائية من أجل مباشرة تحقيقات ناجحة في مجال تقنية المعلومات. وقد اقترن بظهور تقنية المعلومات مشكلات خاصة ومستحدثة وعلى سبيل المثال التفتيش والتحفظ على المعلومات والزام الشاهد باسترجاع وكتابة المعلومات والحق في مراقبة وتسجيل البيانات المنقولة بواسطة أنظمة الإتصالات البعدية وجمعها وتخزينها وضم المعلومات الأسمية إلى

---

[6] Dr. j. Francillon, Les crimes informatiques ET dautres crimes dans le domaine de la technologie informatique en france Rev. int pen, 1990, vol 64, p. 293.

[7] في إحدى الوقائع الشهيرة تعرض بنك Marchant bank city في بريطانيا لنقل 8 مليون جنيه من أحد أرصدته إلى رقم حساب في سويسرا، وقد تم القبض على الفاعل اثناء محاولته سحب المبلغ المذكور ولكن البنك بدل الإدعاء على الفاعل قام بدفع مبلغ مليون جنيه له بشرط عدم إعلان الآخرين عن جريمته وشريطة اعلام البنك عن الآلية التي نجح من خلالها باختراق نظام الأمن الخاص بحاسوب البنك الرئيسي.
راجع في ذلك: يونس خالد عرب مصطفى، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير مقدمة إلى الجامعة الاردنية 1994، ص 72.

[8] وعلاوة على ذلك فإن غالبية الإجراءات الجنائية لا تكون كافية ولا مناسبة لأغراض التحقيق والحكم في هذا النمط من أنماط الجرائم. ومؤدي ذلك فيبدو من الضروري إيجاد اجراءات لديها القدرة على الملاءمة مع المتطلبات الحديثة التي تفرضها تكنولوجيا المعلومات.
راجع في ذلك: Internet: I' La Cniminamite informatique sure.

الدعوى الجنائية. وأهم ما يميز جرائم نظم المعلومات صعوبة إكتشافها وإثباتها وهي صعوبة يعترف بها جميع الباحثين في هذا المجال علاوة على ما تتميز به إجراءات جمع الادلة فـي هذا المجال من ذاتية خاصة.

ومجموعة الأعمال التي يرى المحقق وجوب أو ملاءمة القيام بها لكـشف الحقيقـة بالنـسبة لواقعة معينة يهتم بها قانون العقوبات هي إجراءات التحقيق. وتنقسم هـذه الإجـراءات إلـى قسمين: قسم يهدف إلى الحصول على الدليل كالتفتيش وسماع الشهود وقـسم يمهـد للـدليل ويؤدي إليه كالقبض والحبس الإحتياطي.

وتسمى المجموعة الأولى: إجراءات جمع الأدلة أما الثانية: فتعرف بالإجراءات الإحتياطيـة ضد المتهم. وسوف يقتصر بحثنا هذا على الإجراءات الخاصة بجمع الأدلة وهذه الإجـراءات تنطوي أيضا على المساس بالحريات وهذا ابرز ما يميزها ولهذا فإنه يجـب النظـر إليهـا بإعتبارها واردة على سبيل الحصر فلا يجوز للمحقق ان يباشر إجـراء اخـر فيـه مـساس بحريات الأفراد ولو كان من شأنه ان يؤدي إلى كشف الحقيقة كاستعمال جهاز كشف الكـذب أو مصل الحقيقة.

وإجراءات جمع الأدلة كما حددها القانون هي : المعاينة، ندب الخبـراء، التفتـيش، وضـبط الأشياء، ومراقبة المحادثات وتسجيلها وسماع الشهود والإستجواب والمواجهة. ولـيس علـى المحقق الإلتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غيـر ملـزم اساسـا لمباشرتها جميعا وانما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقـضي به المصلحة وما تسمح به هذه الظروف وسوف نوضح في مجال جمع الأدلة ما يلي:

- أولا: معاينة مسرح الجريمة والمعلوماتية.
- ثانيا: التفتيش في مجال الجريمة المعلوماتية.
- ثالثا: الشهادة في الجريمة المعلوماتية.
- رابعا: الخبرة في مجال الجريمة المعلوماتية.
- خامسا: الضبط في مجال الجريمة المعلوماتية.

- **أولا : معاينة مسرح الجريمة المعلوماتية:**

يقصد بالمعاينة فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالتـه[9]، كمعاينـة مكـان إرتكاب الجريمة أو أداة المعاينة قد تكون إجراء تحقيق لإثبات ما بالجسم من جراح وما على الثيـاب من دماء أو ما بها من مزق أو ثقوب.

[9] توجب المادة 35 من قانون الإجراءات الجزائية الإماراتي على مأموري الضبط القضائي وعلى مرؤوسيهم إجـراء المعاينـة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم أو التي يعملون بها بأي كيفية كانت وتقضي المادة 43 من القانون ذاته بأنـه علـى مأموري الضبط القضائي في حالة التلبس بجريمة أن ينتقل فورا لمحل الواقعة ويعاين الاثار المادية للجريمة ويحافظ عليها ويثبت

ويلاحظ أن المعاينة قد تكون إجراء تحقيق أو إستدلال، ولا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال وإذا اقتضت دخول مسكن أو له حرمة خاصة كانت إجراء تحقيق[10].

والمعاينة جوازية للمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أو لم يطلبوها. ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية[11]. ومرد ذلك إلى اعتبارين:

1. أن الجرائم التي تقع على نظام المعلومات والشبكات قلما يترتب على إرتكابها آثار مادية.
2. أن عدد كبيرا من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة إرتكاب الجريمة وإكتشافها مما يهيء الفرصة لحدوث تغيير أو اتلاف أو عبث بالآثار المادية[12] أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعاينة وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي:

- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل صورة.

- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الإتصال

حالة الأماكن والأشخاص وكل ما يفيد في كشف ا لحقيقة... وعليه إخطار النيابة العامة فورا بإنتقاله وعلى النيابة العامة الانتقال فورا إلى محل الواقعة بمجرد إخطارها بجناية متلبس بها.
كما تنص المادة 90 من قانون الإجراءات الجنائية المصري على أنه ينتقل قاضي التحقيق إلى أي مكان كلما رأى ذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة ماديا وكل ما يلزم إثبات حالته والمقصود بهذا النص تيسير مهمة المحقق وتمكنه من انجاز التحقيق بالسرعة اللازمة قبل ان تندثر معالم الجريمة أو تطمس أدلتها فيتعذر الوصول إلى الحقيقة بعد ذلك.

[10] أنظر في ذلك: د. عوض محمد – قانون الإجراءات الجنائية – الجزء الاول 1989 مؤسسة الثقافة الجامعية ص 470 وما بعدها.

[11] أنظر في ذلك: د. محمد عنب معاينة مسرح الجريمة – رسالة دكتوراه أكاديمية الشرطة – كلية الدراسات العليا القاهرة – 1988 ص 13 وما بعدها.

[12] تنص المادة 266 عقوبات إتحادي فتقضي بأن يعاقب بالحبس كل من غير بقصد تضليل القضاء حالة الأشخاص أو الأماكن أو الأشياء أو أخفى أدلة الجريمة أو قدم معلومات كاذبة تتعلق بها وهو يعلم عدم صحتها كما تنص المادة 286 من القانون ذاته على أن من أخفى أو أوى بنفسه أو بواسطة غيره شخصا فر بعد القبض عليه أو متهما في جريمة أو صادرا في حقه أمر بالقبض عليه، وكذلك كل من أعانه بأي طريقة كانت على الفرار من وجه العدالة مع علمه بذلك يعاقب طبقا للأحوال الاتية...) وتقضي المادة 287 من ذات القانون أيضا بأن من علم بوقوع جريمة وأعان مرتكبيها على الفرار من وجه العدالة بإخفاء دليل من أدلة الجريمة... أو أعانه بأية طريقة أخرى يعاقب طبقا للأحوال الأتية...) كما تنص المادة 145 عقوبات مصري على أنه كل من علم بوقوع جناية أو جنحة أو كان لديه ما يحمل على الإعتقاد بوقوعها وأعان الجاني بأية طريقة كانت على الفرار من وجه القضاء إما بإيواء الجاني المذكور وإما بإخفاء أدلة الجريمة أو بتقديم معلومات تتعلق بالجريمة وهو يعلم بعدم صحتها أو كان لديه ما يحمله على الإعتقاد بذلك يعاقب...".

ونوع الجهاز الذي تم عن طريقة الولوج إلى النظام أو الموقع أو الدخول معـه فـي حوار.

- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكـن أجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.

- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء إختيارات للتأكد من خلـو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسلجة.

- التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربـون المستعملة والشرائط والأقراص الممغنطة وغير السليمة أو المحطمة وفحصها ورفـع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات[13].

- اعداد خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على ان تكون الخطة موضحة بالرسومات وتتم مراجعتها مع اعضاء الفريق قبل التحرك مـع الأخذ في الإعتبار قاعدة smeac العسكرية والتي تعنـي حالـة situation الرسـالة mission التنفيذيـة execution المـداخل والمخـارج avenues of approach والاتصالات communication وهي ملائمة للأجهزة الأمنية وأجهزة تنفيذ القـوانين فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم بالتحقيق فيها، وعدد المتورطين فيه أما الرسالة فهي تحدد الهدف من الغارة والتنفيذ يعنـي كيفيـة أداء المهمـة أمـا المداخل والمخارج فإن معرفتها ضرورية وهي تختلف من جريمة لأخرى وتحـسب وفقا لمكونات طريق التحقيق بينما يأتي عنصر الإتصالات لضمان الـسرية وسـلامة التعامل وتبادل المعلومات اثناء عملية الغارة.

وبعد وصول الفريق إلى مسرح الجريمة أو مكان الغارة يتم التـأمين والـسيطرة علـى المكان والبدء في التفتيش على النحو التالي :

أ- السيطرة على المناطق المحيطة بمسرح الجريمة أو مكان الإعارة وذلك عـن طريـق إغلاق الطرق والمداخل.

---

13 راجع في ذلك : د. هشام محمد فريد رستم.

ب- السيطرة على الدائرة المحيطة بمكان الإغارة بوضع حراسات كافية لمراقبة التحركات داخل الدائرة ورصد الإتصالات الهاتفية من وإلى مكان الإغارة مـع إبطـال أجهـزة الهاتف النقال.

ج- تأمين موقع الغارة والسيطرة على جميع أركانها ومنافذها والتحفظ علـى الأشـخاص الموجودين.

د- تحديد أجهزة الحاسب الآلي الموجودة في مكان الإغارة وتحديد مواقعها بأسرع فرصة ممكنة وفي حالة وجود شبكات إتصالات يجب البحث عن خادم الملـف file server لتعطيل حركة الإتصالات.

ه- يوضع حرس على كل جهاز حتى لا يتمكن أحد المتهمين من إتلاف المعلومات مـن على البعد أو من جهاز آخر داخل المبنى.

و- اختيار مكان لمقابلة المتهمين والشهود على أن يكون المكان بعيدا عن اجهزة الحاسب الآلي[14].

- **ثانيا : التفتيش في مجال الجريمة المعلوماتية:**

التفتيش في قانون الإجراءات هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنهـا وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة وقد احـاط القـانون هـذا التفتيش بضمانات عديدة ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعية قد يكـون متعلقـا بالمتهم أو بغيره وهو في كل أحواله جائز مع إختلاف في بعض الشروط[15].

** وسوف نقسم الدراسة إلى :

1. مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش.
2. ضوابط تفتيش نظم الحاسب الآلي.

1. مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش:

يتكون الحاسب الآلي من مكونات مادية Hard Ware مكونات منطقية Soft ware كما أن له شبكات اتصالات بعدية سلكية ولا سلكية سواء على المستوى المحلي أو المستوى الدولي فهل تخـضع هـذه المكونات للتفتيش؟

---

[14] راجع في ذلك : د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمر القانون والإنترنت بتاريخ 3 مايو 2000 لجامعة الإمارات ص 30.

[15] راجع في ذلك : د. عوض محمد جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية.



أ- مدى خضوع مكونات الحاسب المادية للتفتيش:

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها للإجراءات القانونية الخاصة بالتفتيش وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو مكان عام أم مكان خاص إذ ان لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونيا في التشريعات المختلفة.

ويجب التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم انها متصلة بحاسب أو بنهاية طرفية terminal في مكان آخر كمسكن لا يخص مسكن المتهم فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال.

ب- مدى خضوع مكونات الحاسب المعنوية للتفتيش:

بالنسبة لتفتيش مكونات الحاسب المعنوية فقد ثار الخلاف بشأن جواز تفتيشها حيث يذهب رأي أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الإلكترونية بمختلف أشكالها.

وفي هذا المعنى نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أي شيء بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إليكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق ان يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية[16].

وتمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة إرتكبت أو يشتبه في ارتكابها أو ان هناك نية في أن يستخدم في إرتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة.

[16] راجع في ذلك : د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، طبعة 1997، دار النهضة العربية.



وهكذا يفسر هذا النص بوضوح على أنه يسمح بضبط بيانات الحاسب غير المحسوسة[17] وهناك على النقيض رأي آخر يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي) وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي (البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب)[18]. ويرى بعض الفقهاء في فرنسا أن النبضات الإلكترونية Electronic Impulse أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح[19] ولذا لا يمكن ضبطه.

وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[20].

وتتركز أذون التفتيش القياسية الصادرة عند التفتيش في إحدى جرائم الكمبيوتر – وبصفة خاصة – على ضبط الوثائق المكتوبة إضافة إلى اجهزة الكمبيوتر وتتضمن هذه الوثائق على وجه التحديد: النسخ الضوئية، مطبوعات الكمبيوتر، فواتير التليفون، سجلات العناوين، المذكرات والمراسلات[21].

ت- مدى خضوع شبكات الحاسب للتفتيش:

ويمكن في الفرض التمييز بين ثلاث إحتمالات:

الإحتمال الأول: إتصال حاسب المتهم بحاسب أو نهاية طرفيه موجودة في مكان آخر داخل الدولة: ويرى الفقه الألماني بشان مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم انه يمكن ان يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع اخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني[22].

---

17 راجع في ذلك: د. هلالي عبد اله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، طبعة 1997، دار النهضة العربية.

18 راجع في ذلك : د. هلالي عبد اللاه أحمد سابق الاشاره إليه.

19 انظر في ذلك:
L informatique J.C.P. 1989 333 no 16. Gassin ® Le droit pénal et L informatique D. 1982. p.38

20 راجع في ذلك: Linda Voloniono ibid, p. 2.

21 أنظر في ذلك: Brucisterling, Ibid. P. 165

22 KASPERSEN (W.K.Henrik): computer crimes and other crimes against information technology in the Netherlands R.I.D.P. 1993. P.479.



كما نص مشروع قانون جرائم الحاسب الآلي في هولندا[23] على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125) وذلك بمراعاة بعض القيود.

الإحتمال الثاني: إتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة، من المتصور طبقا لهذا الإحتمال أن يقوم مرتكبو الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الإتصال البعيدة بهدف عرقلة سلطات الإدعاء في جميع الأدلة، ولمواجهة هذا الإحتمال نص مشروع قانون جريمة الحاسب الآلي بهولندا أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأماكن وبما ينطوي عليه تفتيش نظام الحاسب المرتبطة حتى إذا كانت موجودة في دولة أخرى ويشترط أن يكون هذا التدخل مؤقتا وأن تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة 125) [24].

ووفقا لما جاء بتقرير المجلس الأوروبي فإن هذا الإختراق المباشر يعتبر انتهاكا لسيادة دولة أخرى ما لم توجد اتفاقية دولية في هذا الشان ويؤيد الفقه الألماني ما جاء بتقرير المجلس الأوروبي حيث ان السماح باسترجاع البيانات التي تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة أخرى وخرقا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في مجال العدالة القضائي، وقد أيد القضاء الألماني هذا الاتجاه حيث اسفر البحث في إحدى جرائم الغش المعلوماتي عن وجود طرفية حاسب في المانيا متصلة بشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها وعندما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة Request for mutual assistance وقد ساور الإعتقاد الشرطة اليابانية بأن مجموعة من المخربين قد أستخدمت أجهزة كمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كل من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر في كل من هاتين الدولتين حتى تتمكن من الوصول إلى جذور هذه العملية الإرهابية[25].

- الإحتمال الثالث: يسمح بالتنصت wireapping والأشكال الأخرى للمراقبة التليفونية في العديد من الدول[26]، حيث يجيز القانون الفرنسي الصادر في 10 يوليو سنة 1991 إعتراض الإتصالات البعدية telem atique بما في ذلك شبكات تبادل المعلومات[27]، ويجوز لقاضي التحقيق في هولندا أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كانت هناك جرائم خطيرة متورطا فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات، وفي الولايات المتحدة الأمريكية

---

23 راجع في ذلك: د. هلالي عبد اللاه احمد سابق الإشارة إليه.

24 راجع في ذلك :
DURHAM (COLO) the emerging structures of ceremonial information law: trcing the contours of anew paradigm general report for the collwium R.I.D.P 1993. p.115.

25 راجع في ذلك : Linda volonino Ibid. p.4

26 راجع في ذلك : DURHAM (COLO) OP. CITP. 113

27 راجع في ذلك : Dr.Jacques Francillon. Op. cit. 304.



يجوز إعتراض الإتصالات الإلكترونية بما فيها شبكات الحاسب بشرط الحصول على إذن تفتيش صادر من القاضي[28].

2. ضوابط تفتيش نظام الحاسب الآلي:

يمكن تقسيم ضوابط تفتيش نظام الحاسب الآلي إلى نوعين:
موضوعية والأخرى : شكلية

- أولا: الضوابط الموضوعية لتفتيش نظام الحاسب الآلي:

وتنحصر هذه الضوابط في:

أ- وقوع جريمة معلوماتية: والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع مرتبط بإستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة[29]. وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا والتي أصدرت قانون إساءة إستخدام الحاسب الآلي computer misuse في 29 يونيو 1990 وفي الولايات المتحدة الأمريكية حيث صدر قانون الإحتيال وإساءة إستخدام الحاسب الآلي سنة 1986 والذي طبق على المستوى الفيدرالي بالإضافة إلى قوانين بعض الولايات المتحدة الأمريكية كقانون ولاية تكساس الصادر في اول سبتمبر سنة 1985 بشأن الدخول غير المشروع في نظام الحاسب وفي فرنسا صدر قانون رقم 19-88 في 55 يناير 1988 وهو الخاص بالغش المعلوماتي والذي تم تعديله مع صدور قانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من سنة 1985.

وقد أدرج المشرع الإماراتي برامج الحاسب ضمن المصنفات الفكرية المحمية بالقانون الإتحادي رقم 40 لسنة 1992 كذلك إعتبر المشرع المصري مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة ضمن المصنفات المشمولة بحماية حق المؤلف المنصوص عليها في المادة الثانية بمقتضى القانون رقم 38 لسنة 1992.

ب- تورط شخص أو أشخاص معينين في إرتكاب الجريمة المعلوماتية أو الإشتراك فيه: ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الإعتقاد بأنه قد ساهم في إرتكاب الجريمة المعلوماتية سواء بوصفه فاعلا لها أو شريكا فيها وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الإمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة المعلوماتية إلى شخص معين سواء بوصفة فاعلا أو شريكا.

ج- توافر أمارات قوية أو قرائن على وجود أشياء أو اجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم، لا يوجد التفتيش إلا إذا توفرت لدى المحقق أسباب كافية على أنه يوجد في

---

28 راجع في ذلك : BRUCISTERLING ibid. p.165.

29 انظر في : د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ص30.

مكان أو لدى الشخص المراد تفتيشه ادوات استخدمت في الجريمة المعلوماتية أو اشياء متحصلة منها.

د- ومحل التفتيش الخاص بنظم الحاسب الآلي هي كل مكونات الحاسب سواء كانت مادية أو معنوية أو شبكات الإتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش.

وتشمل المكونات المادية للحاسب وحدة الإدخال ووحدة الذاكرة الرئيسة ووحدة الحساب والمنطق و وحدات الإخراج وأخيرا وحدات التخزين الثانوي.

كما تنقسم المكونات المادية المعنوية للحاسب الآلي إلى الكيانات المنطقية الأساسية أو برامج النظام والكيانات المنطقية التطبيقية أو برامج التطبيقات بنوعيها برامج التطبيقات سابقة التجهيز وبرامج التطبيقات طبقا لإحتياجات العميل، ويستلزم الحاسب بمكوناته سالفة الذكر مجموعة من الاشخاص لديهم خبرة ومهارة في تقنية نظم المعلومات وهم مشغلو الحاسب وخبراء البرامج سواء كانوا مخططي برامج تطبيقات ام كانوا مخططي برامج نظم ومحليين ومهندسي الصيانة والإتصالات ومديري النظم المعلوماتية.

- **ثانيا: الضوابط الشكلية لتفتيش نظم الحاسب الآلي:**

أ- الأسلوب الآلي لتنفيذ التفتيش في نظم الحاسب الآلي: نظم القانون الأمريكي أسلوب تنفيذ التفتيش في نظم الحاسب الآلي وذلك على النحو التالي:

تقتحم قوات الشرطة المكان بصورة سريعة ومن كافة منافذه في آن واحد وذلك بإستخدام القدر الأعضم من القوة بإفتراض أن هذا التكتيك يقلل من إحتمالية وقوع إصابات بين صفوف رجال الشرطة.

يتم إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر المتواجدة في المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أي دليل إلكتروني، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كمبيوتر، ودائما ما تكون غرفة المعيشة ويوضعوا تحت حراسة مشددة، وفي هذه الخطوة يتم تقديم التفتيش الصادر من النيابة إليهم ويتم تحذيرهم بأن كافة أقوالهم ستحسب عليهم منذ هذه اللحظة وقد تؤخذ بمثابة دليل إدانه ضدهم ودائما ما سنجد لدى العديد منهم الكثير من الحديث وخاصة إذا ما كانوا أولياء أمور غافلين عن حقيقة ما يحدث بمنزلهم، وفي مكان ما من المنزل، سنجد النقطة الساخنة – جهاز كمبيوتر متصل بخط تليفون أو ربما نجد أكثر من جهاز وأكثر من خط في المنزل الواحد، وعادة ما تكون هذه النقطة الساخنة داخل غرف النوم الخاصة بأحد الأبناء المراهقين.

توضع النقطة الساخنة في عهدة فريق يضم اثنين من العملاء (مكتشف ومسجل) ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريبا متقدما على نظم المعلومات ودائما ما يقوم بهذا الدور العميل المعني بالقضية والذي عاصرها منذ البداية واستصدر إذن التفتيش الخاص بها من القاضي فهذا الشخص يعرف تماما الشيء أو الأشياء التي يبحث عنها ويتفهم طبيعتها تماما ولن نتجاوز إذا ما قلنا أنه هو الذي يقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات الإسطوانات.... الخ.

أما المسجل فيتولى تصوير كافة الأجهزة والمعدات على ذات الكيفية التي تم ضبطها عليها، ويقوم المسجل كذلك بتصوير كافة الغرف الأخري الموجودة بالمنزل حتى لا يدعي احد المجرمين الماكرين ان الشرطة قد سرقت منزله أثناء التفتيش.

ب- فريق التفتيش: هو الفريق المعني بإجراءات التحقيق وهو جزء داخل فريق الإغارة الذي يضم بجانب فريق التفتيش والضبط رجال الحراسات والأمن وقوات الحماية والتأمين ورجال المباحث والمراقبة السرية والمعاونين من العمال والعمال المهرة والسائقين وخبراء مسرح الجريمة العادية الملائمين لجريمة موضوع التحقيق، ويتكون فريق التفتيش والضبط من:

- **المشرف على التحقيق:**

والذي يجب أن يكون من ذوي الخبرات الطويلة في مجال التحقيق الجنائي في الجرائم المعقدة ويتولى المشرف إدارة العمل في مسرح الجريمة وتوزيع المهام على أعضاء الفريق.

- **فريق أخذ الإفادات:**

ويحدد عدد أعضاء هذا الفريق حسب حجم الجريمة والمتورطين فيها وعدد الشهود الذين قد يتواجدون في مسرح الجريمة وعليه قد يكون الفريق من شخصين أو اكثر.

- **فريق الرسم والتصوير:**

ويضم شخصا أو أكثر يقومون برسم الخرائط الكروكية لمسرح الجريمة وتحديد موقع الأجهزة والملفات والأشخاص والتقاط الصور الفوتوغرافية والتصوير بالفيديو، مع مراعاة أن يتم تنبيه جميع العاملين في مسرح الجريمة عند إستعمال الفيديو تحسبا لتسجيل أصوات المشاركين في التفتيش.

- **فريق التفتيش العملي:**

ويضم شخصا واحدا أو أكثر حسب الأحوال ويتولى هذا الفريق عملية البحث والتدقيق على مسرح الجريمة وفقا للنظم الفنية التي تتبع في تفتيش الاماكن وتفتيش مسرح الجريمة ويقوم هذا

الفريق بالمرور على جميع الغرف والمخازن ويفحص المخازن والمخابئ وليس من الضروري ان يكون اعضاء هذا الفريق من خبراء الحاسب ولكن يفضل ان يتم تنويرهم بالأشياء التي ينبغي البحث عنها.

- فريق التأمين والقبض:

ويعني هذا الفريق بالسيطرة أمنيا على مسرح الجريمة وضـبط مخارجهـا ومنافـذها وحركـة الموجودين بالمبنى والمباني المجاورة لمسرح الجريمة، وتنفذ عملية القبض على المشتبه فـيهم واحتجازهم وفق ما يأمر به المشرف ويتكون هذا الفريق من رجال الأمن بالزي الرسمي.

- فريق ضبط وتحرير الأدلة:

ويضم هذا الفريق أثنين أو أكثر من خبراء الحاسب الآلي يتولون ضـبط وإدخـال المعلومـات المضبوطة في الحاسب الآلي وتصنيف الأدلة وتحريزها فـي الـصناديق ووضـع العلامـات الموضحة عليها ويقوم هذا الفريق بنقل أجهزة الحاسب الآلي المضبوطة بعد أجـراءات الرسـم والتصوير ويجب ان يكون من بين اعضاء هذا الفريق شخصان على الاقل احدهما محقـق فـي مجال الحاسب الآلي، والثاني خبير في الحاسب الآلي مدرب على التعامل مـع الأدلـة وطـرق تقييمها.

- خبير مسرح الجريمة العادية:

ويتم اختيارهم حسب الحال وقد يحتاج المحقق في بعض جرائم الحاسب كامل أعـضاء الفريـق أو بعضهم مثل خبراء البصمات، المهندسين، خبراء المتفجرات... الخ.

- **ثالثا: الشهادة في مجال الجريمة المعلوماتية:**
- **تعريف الشهادة وأهميتها:**

- الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سـواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها[30]، وللشهادة في مجال الإجراءات اهمية بالغة لأن الجريمة ليست تصرفا قانونيا ولكنها عمل غير مشروع يجتهد الجاني في التكتم عند ارتكابه ويحرص على إخفائه عن الناس.

ولهذا فأن العثور على شاهد يعتبر مكسبا كبيرا للعدالة ومن هنا جاءت قاعدة عدم رد الشهود.

[30] تعرف محكمة النقض ا لمصرية الشهادة بأنها تقرير لشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه (نقض 1976/1/25 أحكام النقض س 27 ص 94 رقم 20 و 1978/2/6 س 29 ص 139 رقم 25 و 1979/4/2 س 27 ص 94 رقم 20 و 2978/2/6 س 29 ص 139 رقم 25و 1979/4/2 س 30 ص 426 رقم 90.



- **تعيين الشهود وأستدعائهم:**

سماع الشهود كسائر أجراءات التحقيق من الامور التقليدية للمحقق فله ان يسمع الشهود أو يستغني عنهم فإذا قرر سماعهم فهو الذي يحدد من يجب الإستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك إلى فطنة المحقق ومرتبط بظروف التحقيق والأصل أن يطلب الخصوم سماع من يرون من الشهود غير أن للمحقق أن يجيبهم إلى طلبهم أو يرفضه وله أن يدعو للشهادة من يقدر أن لشهادته أهمية بل له ان يسمع شهادة أي شاهد يتقدم من تلقاء نفسه، ومن المبادء المستقرة أن الشاهد لا يرد ولو غلب على الظن أنه لن يتحرى الصدق في شهادته سواء كان ذلك راجعا لانحطاط في خلقه أو لوجود صلة مودة أو لعداوة بينه وبين المتهم تجعله يميل له أو ضده.

- **المقصود بالشاهد في الجريمة المعلوماتية:**

الشاهد في الجريمة المعلوماتية الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي وذلك تمييزا له عن الشاهد التقليدي ويشمل الشاهد المعلوماتي بهذا المفهوم عدة طوائف من اهمها:

1. القائم على تشغيل الحاسب الآلي"

وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز وإستخدام لوحة المفاتيح في ادخال البيانات كما يجب ان تكون لديه معلومات عن قواعد كتابة البرامج[31].

2. المبرمجون:

وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين:

- الفئة الأولى: هم مخططو برامج التطبيقات.
- الفئة الثانية: هم مخططو برامج النظم.

حيث يقوم مخططوا برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، اما مخططو برامج النظم فيقومون بإختبار وتعديل وتصحيح برامج نظام

[31] انظر في ذلك : د. محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، القاهرة مطابع المكتب المصري الحديث سنة 1991 ص 23.



الحاسب الداخلية اي انه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والاجزاء الداخلية التي تتحكم في وحدات الادخال والاخراج ووسائط التخزين بالاضافة إلى ادخال اي تعديلات أو اضافات لهذه البرامج.

3. المحللون:

المحلل وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة وأستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما سمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

4. مهندسو الصيانة والإتصالات:

وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

5. مديرو النظم:

وهم الذين يوكل لهم أعمال الأدراة في النظم المعلوماتية32.

- ويحصل قانون الدليل الخاص بولاية كاليفونيا شهود الجريمة المعلوماتية في:
- محلل النظم الذي صمم وحدد برنامج الكمبيوتر الذي انتج الدليل.
- المبرمج الذي قام بتحرير البرنامج واختباره.
- المشغل الذي يقوم بتشغيل البرامج.
- طاقم عمليات البيانات الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة).
- أمناء مكتبة الأشرطة الذين يتحملون مسؤولية توفير الأشرطة أو الأسطوانات التي تشتمل على البيانات المصدرية الصحيحة.
- مهندس الصيانة الألكترونية الذي يقوم على صيانة الجهاز الاصلي والتأكد من عمله بصورة صحيحة.
- موظفو المدخلات والمخرجات والمسؤولون عن معالجة المدخلات المستخدم في تنفيذ برامجه.
- المستخدم النهائي الذي يمد بالمعلومات المدخلة ويصرح بتنفيذ برامج الكمبيوتر ويستخدم نواتجها[33].

---

32 أنظر في ذلك: د. محمد فهمي طلبة، الحاسبات الإلكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصري الحديث سنة 1992.

33 بحث مقدم من مركز البحوث بشرطة دبي عام 1998، للامارات العربية المتحدة.

- **التزامات الشاهد المعلوماتي:**

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهريـة لازمـة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والافصاح عن كلمات المرور والشفرات؟

** هناك اتجاهان في هذا الصدد:

- **الاتجاه الاول:**

ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة ان يقوم بطبع ملـف البيانـات أو الافصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلـى هـذا الإتجـاه الفقـه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسـب علـى اسـاس أن الالتزام بإداء الشهادة لا يتضمن هذا الواجب[34].

وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الأفصاح عن كلمات المرور الـسرية أو كـشف شفرات تشغيل البرامج المختلفة[35].

- **الاتجاه الثاني :**

ويرى أنصار هذا الإتجاه أن من بين الإلتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانـات أو الافصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى أتجاه في الفقه الفرنسي ان القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الإلتزام بتقديم شهادتهم (المواد 62، 109، 138 من قـانون الإجـراءات الجنائية الفرنسية) ومن ثم يجب عليهم الافصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة[36].

وفي هولندا يتيح مشروع قانون الحاسب الآلي لسلطات التحري والتحقيق أصدار الأمر للقائم بتـشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المـرور الـسرية والشفرات الخاصة بتشغيل البرامج المختلفة وإذا وجدت بيانات مشفرة أو مرمزة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها، يتم تكليف القائم على تشغيل النظام المعلوماتي بحـل رموز هذه البيانات[37].

---

34 انظر في ذلك :
- Mohrenschloager (Manfred): Computer crimes and other crimes against information technology in Germany "R.I.D.P 1993 P. 351.

35 انظر في ذلك:
Erman (Sahir) "les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie R.I.D.P. 1993, p.64

36 راجع في ذلك: Dr.Jacques francillon op. cit. p. 309

37 انظر في ذلك : Kasbersen op. cit. p.496

وفي اليونان يمكن الحصول من القائم على تشغيل نظام الحاسب على كلمة المرور السرية للولوج في نظام المعلومات كما يمكن الحصول منه على بعض الايضاحات الخاصة بنظامه الامني لكن ليس على الشاهد اي التزام بالنسبة لطباعة ملفات بيانات مخزنة في ذاكرة الحاسب وذلك لأنه يجب ان يشهد على معلومات حازها بالفعل وليس الكشف عن معلومات جديدة (المادة 223 فقرة 1 إجراءات جنائية يونانية).

- **رابعا : الخبرة في مجال الجريمة المعلوماتية:**

ندب الخبير أو مبررات ندب الخبير وإجراءاته: يرى المحقق في بعض الأحيان ضرورة الإستعانة بالخبير لإيضاح مسألة تستعصى ثقافته العامة عن فهمها كتحديد سبب الوفاة أو ساعتها أو رفع بصمة وجدت في مكان الجريمة أو فحص سيارة لبيان ما فيها من خلل وتكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتية نظرا لأن الحاسبات وشبكات الإتصال بينها على أنواع ونماذج متعددة كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها وإستعابها ويمكن القول بصفة عامة بأنه لا يوجد حتى الأن خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكتها كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[38].

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة[39]، وللمحقق في اي وقت إلى أن ينتهي التحقيق – أن يندب من يأنس فيه الكفاءة الفنية اللازمة للاستعانة بخبرته.

وندب الخبير من سلطات المحقق فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم إذا طلبوا ندب الخبير.

يحدد المحقق للخبير مهمته والميعاد الذي يقدم فيه تقريره وعليه أن يحلفه اليمين على أن يبدي رأيه بالذمة وهذا الأجراء جوهري يترتب على أغفاله بطلان عمل الخبير[40]. والاصل ان يباشر الخبير عمله في حضور المحقق وتحت إشرافه والأستثناء أن يتم ذلك في غيابه.

---

38 راجع في ذلك :

- Philip M. Stanley computer crime investigation and investigators computer & security Nort Holland 1986, pp. 310 – 311.

مشار إليه في : د. هشام محمد فريد رستم، مرجع سابق الأشارة إليه.

39 راجع في ذلك : Investigation computer crime
Franklin Clark den Dilbert p. 147

40 نقض مصري 1926/12/26 المحاماة س 7 ص 789 و 1972/2/8 س 8 ص 1958 و 1972/3/1 مجموعة القواعد القانونية ج 4 ص 52 رقم 43.

وللخصوم حق الحضور اثناء عمل الخبير ويجوز مع ذلك ان يباشر الخبير عمله في غياب الخصوم وأن يمنعهم كذلك من الحضور إذا كان للمنع سبب، ويعد الحصول على المستندات خلال عملية التفتيش امرا سهلا حيث يمكن التعرف عليها بالرؤية ولن يحتاج المحقق لأي مساعدة من قبل الخبراء وهذه المستندات مثل: أدلة عمل النظام، سجلات إدارة الكمبيوتر، وثائق البرامج، السجلات، صيغ مدخلات البيانات والبرامج، وكذلك صيغ مخرجات الكمبيوتر المطبوعة ويتم التخطيط على هذه المستندات ويمكن تحديد ما إذا كانت كاملة، أصلية، أو صورا من خلال استجواب القائمين على حفظها.

وقد يكون التخطيط على المواد المتعلقة بوسائل الكمبيوتر الأخرى أمرا اكثر تعقيدا مثل : الاشرطة الممغنطة الأسطوانات، البرامج ويحتاج إلى معونة احد الخبراء الموثوق فيهم حتى يتمكن المحقق من الالمام بمحتويات الاشرطة أو الاسطوانات دون احداث اي تغيير فيها.

وبالطبع، فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد امرا بالغ التعقيد ويحتاج إلى وجود خبير[41]. وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:

- اولا : وصف:

أ- تركيب الحاسبات وصناعته وطرازه ونوع نظام التشغيل واهم الأنظمة الفرعية التي يستخدمها بالأضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير.... الخ.
ب- طبيعة بيئة الحاسب أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الإتصالات وتردد موجات البث وأمكنة اختزانها.
ج- الموضع المحتمل لأدلة الأثبات والشكل أو الهيئة التي تكون عليها.
د- أثر التحقيق من الوجهة الإقتصادية والمالية على المشاركين في إستخدام النظام.

- ثانيا: بيان

أ- كيف يمكن عند الإقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو الحاق ضرر بالأجهزة.
ب- كيف يمكن عند الإقتضاء نقل أدلة الإثباتات إلى أوعية ملائمة بغير ان يلحقها تلف.
ج- كيفية تجسيد الأدلة في صورة مادية بنقلها إذا امكن إلى اوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع اثبات ان المسطور على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة[42].

---

41 راجع في ذلك:
بحث مقدم من مركز البحوث والدراسات بشرطة دبي – الإمارات العربية المتحدة، بعنوان جرائم الكمبيوتر سنة 1998 ص 2.

42 انظر في ذلك :

- **خامسا: الضبط في مجال الجريمة المعلوماتية:**
- معنى الضبط وطبيعته:

يقصد بالضبط في قانون الإجراءات وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث طبيعته القانونية قد يكون من إجراءات الإستدلال أو التحقيق.

وتتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريدة من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الإستيلاء عليها دون الإعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال.

- **محل الضبط:**

الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء اما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق وإذا كان قانون الاجراءات يتحدث في بعض التصرف عن ضبط الأشخاص واحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماما عن ضبط الاشياء.

ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك فإنه يستوي ان يكون الشيء المضبوط مملوكا للمتهم أو لغيره، والقاعدة أن الضبط لا يرد إلا على شيء مادي أما الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحته أن يكون الشيء مفيدا في كشف الحقيقة فكل ما يحقق هذه الغاية يصح ضبطه.

والأدلة المادية التي يجوز ضبطها في الجريمة المعلومايتة والتي لها قيمة خاصة في إثبات جرائم الحاسب الآلي ونسبتها إلى المتهم هي :

1. الورق : كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي، مما قلل حجم الأوراق والملفات ومع ذلك نجد ان الكثيرين يقومون بطباعة المعلومات print out لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات موضوع الجريمة وأجهزة الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبق قدرا كبيرا من الأوراق في وقت قصير عليه يعتبر الورق من الأدلة التي ينبغي الإهتمام بها في البحث وتفتيش مسرح الجريمة والورق أربعة أنواع :

أ- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصور للعملية التي يتم برمجتها.
ب- أوراق تالفة تتم طباعتها للتأكد ومن ثم إلقاؤها في سلة المهملات.

د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلآت الحديثة، 1994.

ج- أوراق اصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.
د- أوراق اساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تلقيها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

2. جهاز الحاسب الآلي وملحقاته: Computer paraphernalia

وجود جهاز حاسب الي مهم للقول بأن هناك جريمة ولاجهزة الحاسب الآلي اشكال وأحجام والوان مختلفة وخبير الحاسب الآلي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية الأخرى وتحديد اسلوب التعامل معه في حالة الضبط والتحريز.

3. الحاسب الآلي، لوحة المفتاح، والشاشة: من السهل التعرف على جهاز الحاسب الشخصي الذي أصبح مألوفا اليوم فهو يتكون من وحدة المعالجة المركزية CUP، لوحة المفاتيح Key board والشاشة Monitor ومع التطورات السريعة التي يمر بها الحاسب الآلي نجد إضافات جديدة مثل المودم والماوس والسماعات والسيرفر، وإذا كنا بصدد الحديث عن الأجهزة الكبيرة فإننا نجد أن اشكالها تتغير بإستمرار خاصة من حيث الحجم والهيكل ومن الضروري اطلاع العاملين في مجال التحقيق على مختلف أشكال اجهزة الحاسب الآلي فور ظهورها.

4. أقراص الليزر: Disks and diskettes

مع جهاز الحاسب آلي شخصي عادي تجد قدرا كبيرا من أقراص الليزر علاوة على أن مراكز الحاسب الآلي في الشركات والبنوك قد تجد فيها الآلاف من الاقراص قد تكون على غلاف القرص بيانات توضح محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة وقد تجد في مكان ما أقراص الليزر ولا تجد معها أجهزة حاسب آلي ومع ذلك يعد جزءا من جريمة حاسب آلي متى كانت محتوياتها عنصرا من عناصر الجريمة.

5. الشرائط الممغنطة Magnetic Tapes

وتستعمل الشرائط الممغنطة عادة للحفظ Backup الاحتياطي وقد تكون في مكان بعيد آمن كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة.

6. لوحة الدوائر: circuit boards and components

7. المودم: Modem

والمودم Modulator /demodulator هي الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال مع بعضها البعض عبر خطوط الهاتف وقد تطورت المودم إلى أجهزة إرسال الفاكس والرد على

المكالمات الهاتفية وتبادل البيانات وتعديلها، وللمودم أشكال وهياكل تتطور مع تطور تقنية صناعة الحاسب الآلي.

8. الطابعات Printers

وللطابعات أنواع منها العادية ومنها طابعات ليزرية منها الملونة ومنها غير ملونة.

9. Pcmcia Cards

وتستعمل بطاقات الـ Pcmcia في أجهزة الحاسب الآلي الـصغيرة النـوت بـوك Notebook واللاب توبLaptop وهي في شكل البطاقات الإئتمانية.

10. البرامج اللينة والمراشد: المراشد Manuals المصاحبة للحاسب الآلي مفيدة في التعـرف علـى الجهاز والبرامج المستعملة فيها.
11. البطاقات الممغنطة وبطاقات الإئتمان القديمة والمواد البلاستيكية المستعملة في إعداد تلك البطاقات تعتبر قرائن للاثبات في جرائم الحاسب الآلي.

كل ذلك يعد أثرا أو جزءا من جسم الجريمة ينبغي البحث عنها وفحصها والإستفادة منها في التحقيـق علما بأن التعامل مع مثل هذ الآثار يحتاج إلى خبرة فنية في مجال الحاسب الآلي ومعرفـة بالقـانون وقواعد البيئة.

الملخص

ظاهرة جرائم الحاسب الآلي ظاهرة إجرامية جديدة مستجدة تقرع في جنباتها أجراس الخطـر لتنبـه مجتمعات العصر الراهنة لحجم المخاطر وهول الخسائر الناجمة عن تلك الظـاهرة الإجراميـة التـي تستهدف الإعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها).

فجريمة الحاسب الآلي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكـون أدوات المعرفـة التقنية وتوجه للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومـات المنقولة عبر نظم وشبكات المعلومات.

وترتب على الإستخدام المتزايد لنظم المعلومات سواء في شكل أموال معلوماتية أو أساليب مـستحدثة إلى نشوء ما يعرف بالجريمة المعلوماتية وهي نتيجة حتمية لكل تطـور علمـي أو تقنـي مـستحدث ويرتكز هذا النوع من الإجرام على محورين أولهما ضد المال والثاني ضد الأشخاص ويستمد نـشاطه من القدرات الهائلة للحاسب الآلي.

لذا يلزم للمجتمع المعلوماتي في مجال قانون الإجراءات الجنائية أن ينشأ قواعد قانونية حديثة بحيـث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق في مجال جرائم الكمبيوتر، وأهم ما يميز جرائم نظم المعلومات صعوبة إكتشافها وإثباتها وهي صعوبة يعترف بها جميع الباحثين في هـذا المجال علاوة على ذلك ما تميز به إجراءات جميع الأدلة في هذا المجال من ذاتية خاصة.

تم توضيح إجراءات جميع الأدلة في هذا البحث من ناحية أنواع الأدلة فـي مجـال جريمـة سـرقة المعلومات، والإشارة إلى مسرح الجريمة والتفتيش في مجال هذه الجريمة والخبرة والضبط في شأنها وشهادة الشهود وقد أصبح لكل شخص يعيش في المجتمع الحق بالإتصال بغيره وتبادل المنافع المعنوية والمادية معه ليس فقط داخل دولته بل كذلك خارجها مع أبناء الدول الأخرى.

A synopsis
The ways to collect the guides
Theft of information stored in Computers

Computer crimes represent a recent up-date phenomenon that implicitly tolls alarm bells to warm the modern societies of the great dangers and enormous losses resulting from such criminal phenomenon that targets the inputs with their vast technology significance (all forms of data, information, and programs).

The computer crime is a technological crime that originates in secret, and is committed by smart criminals who have the means of technological know-how which is directed to violate the right of access to information conveyed through information systems network.

The ever-increasing use of information systems, either in the from of informatics or unprecedented methods, or the emergence of the so-called information crime, is an inevitable outcome of every new scientific or technological development. This type of incrimination is based on two axes, the first against the money and the second against the person. It derives its activity from the formidable potentials of the computer.

Then the light was shed upon the legal nature of the programs. Firstly, their classification in accordance with the Civil law, and existing relation between the intellectual property and the programs.

The study of the theft crimes from the point of view of its relation with the system of power-driven processing of information is distinguished by a great deal of accuracy, rather it represents the most difficult subject of study, as it require the analysis of the elements of that system in order to know the disposition of each element to become the subject of theft.

Due to the easy way of moving the information in the domain of information technological systems, it is possible to commit a crime through a computer existent in a certain country, while the consequences of such criminal act appear in another country.